

Appendix F

Informix Security CHECKLIST

Topic: Database Management System

SubTopic: File System Security

Objective 205

Verify that application files are stored on the recommended drives/devices.

Rationale:

To protect the system database since it contains all system data and to protect the audit database.

DII COE SRS Requirement:

Test Actions:

Step: 1

Required Action:

Expected Results:

Comments:

Storing the physical and logical logs on different disks minimizes the chances of creating an I/O bottleneck.

Topic: Database Management System

SubTopic: File System Security

Objective 206

Verify that application executables and configuration files are not in the same directory path as the application data files.

Rationale:

To separate the software and data files.

DII COE SRS Requirement:

Test Actions:

Step: 1

Required Action:

Expected Results:

Comments:

Separates the software and data files.

Topic: Database Management System

SubTopic: File System Security

Objective 207

Verify the application directory is owned by the proper user and the file permissions are set correctly.

Rationale:

Limits access to application files.

DII COE SRS Requirement:

Test Actions:

Step: 1

Required Action:

Check the permissions on the file `$INFORMIXDIR/etc/sqlhosts`.

Expected Results:

Only user informix should have read and write permissions on it.

All other users should have write permissions.

Comments:

The file `sqlhosts` contains the name of each database server and aliases to which the clients can connect. For each database server name and alias, it also specifies the protocol that a client must use to connect to the database server. Only informix account has update permissions to the configuration files (`sqlhosts` and `onconfig.std`).

Topic: Database Management System

SubTopic: File System Security

Objective 208

Verify that a group has been defined for database users and that only authorized users are members of this group.

Rationale:

Limits database access to database users only.

DII COE SRS Requirement:

Test Actions:

Step: 1

Required Action:

View the /etc/groups file to verify that a group has been created for informix users.

Expected Results:

There should be a group created for informix users.

Comments:

Topic: Database Management System

SubTopic: File System Security

Objective 209

Verify that all database application files have the correct group permissions.

Rationale:

Restricts access to the application files.

DII COE SRS Requirement:

Test Actions:

Step: 1

Required Action:

Type in the following command:

```
#ls -la $INFORMIXDIR
```

Expected Results:

This file should have only group read/execute permissions. The group permissions should be read/execute for all files in the \$INFORMIXDIR directory.

Comments:

Only informix account has update permissions to the control files.

Topic: Database Management System

SubTopic: I & A

Objective 210

Verify that NULL passwords are not used for database level logins.

Rationale:

Having a password provides extra protection and user authentication.

DII COE SRS Requirement:

Test Actions:

Step: 1

Required Action:

Attempt to login into the Informix database using a null password.

Expected Results:

Login should fail.

Comments:

Do not use null passwords/guest accounts. Informix uses the operating system username and password for authentication of a given user. Having a password provides extra protection.

Topic: Database Management System

SubTopic: I & A

Objective 224

Verify that a single remote login account to the database application is not used for multiple remote users.

Rationale:

It reduces individual accountability on the server. Audit actions can be traced only to the local server login.

DII COE SRS Requirement:

Test Actions:

Step: 1

Required Action:

Expected Results:

Comments:

Reduces individual accountability on the server. Audit actions can be traced only to the local server login.

Topic: Database Management System

SubTopic: Access Control

Objective 251

Verify that access to the database privileged account is restricted.

Rationale:

Restricts access to the database.

DII COE SRS Requirement:

Test Actions:

Step: 1

Required Action:

Attempt to assume the privileged informix users role as a non-privileged user.

Expected Results:

Attempt should fail.

Comments:

Topic: Database Management System

SubTopic: Access Control

Objective 214

Determine if separation of user roles (e.g., SSO or SA) is enforced, and if so, ensure that different individuals have been assigned to these roles.

Rationale:

Role separation is an enhanced-security feature designed to provide checks and balances to administrative responsibilities.

DII COE SRS Requirement:

Test Actions:

Step: 1

Required Action:

Check to see that environmental variable INF_ROLE_SEP is set and groups ix_dbssso and ix_aao are defined.

Expected Results:

Comments:

Role separation is enforced if environment variable INF_ROLE_SEP is set and a group is specified for DB_SSO and AAO, ix_dbssso and ix_aao. If the file "\$INFORMAIXDIR/dbssodir/seccfg" has "ixuser=*" then all users have access to the database server. If "ixusers=engineer" then only the engineering group has access to the server. Role separation in OnLine is accomplished by requiring members of different UNIX operating system user groups to perform unique administrative tasks in running OnLine. The application Administrator may be given the privileges of a Database Administrator for databases accessed by the application. Having a separate database owner for the shared database provides individual accountability.

Topic: Database Management System

SubTopic: Access Control

Objective 216

Verify that no database users are given the "grant with grant option" permission to database objects. If necessary, verify any users that have this permission are valid privileged database users.

Rationale:

To restrict the transmittal of access to database objects.

DII COE SRS Requirement:

Test Actions:

Step: 1

Required Action:

Use the "INFO ACCESS table_name" command to display user access privileges for a specified table. In the query interface of the DBACCESS utility, issue the query:

```
SELECT * FROM systabauth
```

Expected Results:

If the value in the column tabauth of system table systabauth is in uppercase it means that privilege has been granted with the "with grant option."

Comments:

The "AS grantor" clause lets you establish a chain of privileges with another user as the source of the privileges.

Topic: Database Management System

SubTopic: Access Control

Objective 218

Verify that the UNIX alias mechanism is not used to treat two or more users as the same user within the database application.

Rationale:

Maintains individual traceability.

DII COE SRS Requirement:

Test Actions:

Step: 1

Required Action:

Expected Results:

Comments:

Using the alias mechanism prevents individual accountability for actions performed under the alias.

Topic: Database Management System

SubTopic: Access Control

Objective 221

Verify that stored procedures and triggers do not inadvertently accelerate general user permissions.

Rationale:

Permission to execute a stored procedure or a trigger gives a user indirect access to underlying database objects.

DII COE SRS Requirement:

Test Actions:

Step: 1

Required Action:

Use the keywords, PRIVILEGES, REFERENCES, or STATUS in the INFO statement to get user access privileges, reference privileges, and status of a specified table. Also the system table sysdepend describes how each view or table depends on other views and tables. The system table sysprocauth describes privilege on a procedure.

Expected Results:

If the value of column "procauth" in the system table "supprocauth" is "E", it means the grantee has execute permission and the ability to grant it to others.

Comments:

When designing stored procedures and triggers and when granting privileges to users to execute these stored procedures and triggers, the ownership chains should be carefully monitored. The user also inherits access privileges of the creator of the stored procedure or the trigger if the owner has WITH GRANT OPTION right for necessary privileges to the underlying objects. Also by using the "AS grantor" clause the ownership chains can be transferred which can make revoking of privileges difficult.

Topic: Database Management System

SubTopic: Access Control

Objective 223

Verify that password and/or network encryption is used to access a remote server.

Rationale:

Having a password or network encryption provides extra protection over the network.

DII COE SRS Requirement:

Test Actions:

Step: 1

Required Action:

Expected Results:

Comments:

Avoid using the capability of remote hosts to access the database server without passwords. The /etc/hosts.equiv and /.rhosts files are optional UNIX files that can be created on the server host machine. They specify which remote hosts and user are trusted and allowed access to the server machine without supplying a password. The database server uses these files to determine whether a remote client should be allowed access to the server without specifying a password explicitly.

Topic: Database Management System

SubTopic: Audit

Objective 222

Verify that application level audits are generated for the vendor recommended events.

Rationale:

Ensures traceability of user actions.

DII COE SRS Requirement:

Test Actions:

Step: 1

Required Action:

Use the "onshowaudit" UNIX command to view data that has been captured into audit logs.

Expected Results:

Informix provides C2 level of auditing.

Comments:

Audit files are created in a directory which the DBA specifies. The files are flat UNIX system files. The files should be owned by root with a Informix groupid and file permissions set to 600.

A series of command line options to create and maintain audit masks are shown in the Informix-OnLine Dynamic Server Trusted Facility Manual Version 7.1 in Chapter 4.

Topic: Database Management System

SubTopic: Recovery Management

Objective 225

Verify that backups of the database can be performed and that they are performed on a regular basis.

Rationale:

Ensures recovery from failures.

DII COE SRS Requirement:

Test Actions:

Step: 1

Required Action:

Expected Results:

Comments:

Different alternatives for recovery management are:

- a. When mirroring is active, the same data is stored on two disks simultaneously.
- b. HDR is the transparent replication of data from a primary server to a secondary server.
- c. Running the database in mode ANSI ensures unbuffered logging, that is the records in the logical log buffer are guaranteed to be written to the disk before the COMMIT statement returns to the application. This prevents loss of committed transaction if the system crashes.

TAPEDEV and LTAPEDEV are archiving parameters in the ONCONFIG configuration file.

Topic: Database Management System

SubTopic:

Objective 249

Determine if the database application uses /tmp directory for temporary storage during execution.

Rationale:

Ensures that deletion of /tmp directory does not inadvertently delete online configuration files.

DII COE SRS Requirement:

Test Actions:

Step: 1

Required Action:

Expected Results:

Comments:

The /tmp directory might contain some configuration files for Informix OnLine. Warn UNIX administrator about cron jobs to routinely delete /tmp files. OnLine creates the inf.servicename and VP.servernameC files in /tmp directory. Some UNIX systems run cron jobs to routinely delete /tmp files. If the files in /tmp are deleted, then OnLine has to be restarted.

Topic: Database Management System

SubTopic:

Objective 250

Verify that any available secure database options were used during database creation, and the correct options are included in database startup and shutdown scripts.

Rationale:

Ensures database is created with the proper security options.

DII COE SRS Requirement:

Test Actions:

Step: 1

Required Action:

Expected Results:

Comments:

All databases use unbuffered logging. Owner naming is enforced. Write a startup and shutdown script and include it in the system startup and shutdown areas. Users do not receive PUBLIC privilege to tables and synonyms by default.